Аладдин

Как создать безопасное рабочее пространство на корпоративном компьютере с ОС Linux

Содержание:

Резюме

Российский рынок находится в самом разгаре перехода на отечественные ИТ-решения. Вызовов, связанных с переходом, великое множество. И перевод рабочих станций сотрудников на ОС семейства Linux не является исключением. Необходимость организации удобного универсального рабочего места сотрудника на базе Linux выделяется на общем фоне за счёт множества технологических сложностей, с которыми сталкивается ИТ-персонал компании. Вопросы совместимости программного обеспечения, адаптации новых прикладных программ или банального отсутствия привычных ИТ-инструментов в среде Linux безусловно важные и актуальные. Однако на первый план при "переезде" на ОС Linux выходит задача защиты информации на новом рабочем месте. В данном документе пойдёт речь о простом и универсальном способе организации безопасного рабочего пространства для пользователя в отечественных ОС на базе Linux.

Требования к современным средствам защиты информации

Сама суть описанной проблемы диктует основные требования организации к выбору инструмента обеспечения безопасности:

Надёжность применяемого метода защиты

По оценкам различных аналитиков в российских офисах доля ноутбуков ежегодно растёт и уже превышает 45% от общего количества рабочих станций. Применяемое средство должно учитывать эту особенность и обеспечивать гарантированную защиту информации даже при работе сотрудника за пределами организации.

Простота внедрения

Специалисты отрасли единогласно рекомендуют использовать при переходе на новые рабочие станции наиболее простые во внедрении и понятные в применении программные средства, потому что это сделает сам переход безболезненным и достижимым в реалистичные сроки.

Универсальность программного средства

Средство защиты должно поддерживать популярные версии ОС семейства Linux, которые производятся российскими вендорами. Обилие отечественных операционных систем и, как следствие, отсутствие широкой поддержки со стороны производителей средств защиты является известной проблемой.

Компания "Аладдин Р.Д." выпустила программное средство Secret Disk для Linux, которое удовлетворяет всем этим злободневным требованиям и позволяет просто и в кратчайшие сроки организовать защищённое рабочее пространство пользователя на рабочей станции под управлением Linux-систем.

Шифрование виртуальных дисков. Почему мы выбрали этот метод защиты?

Очень часто клиенты обращаются к нам с вполне понятной просьбой – необходимо зашифровать данные в среде Linux аналогичными инструментами, которые существуют в Windows. Это связано с тем, что большинство пользователей привыкли к работе с Windows и сформировали удобный и привычный для себя способ работы с особо защищаемыми данными.

Мы решили при создании первой версии Secret Disk для Linux адаптировать механизмы защиты под уже знакомый для пользователей формат. А именно – организовать возможность хранения особо важной и конфиденциальной информации на защищённом виртуальном диске.

В целом создание виртуальных дисков в Windows – понятная и крайне популярная среди пользователей функция. Виртуальный диск экологично изолирует важные рабочие папки и файлы от остальной файловой структуры. Это сильно повышает удобство работы с данными для мобильных сотрудников, использующих свой рабочий ноутбук вне офиса. А как мы помним, доля ноутбуков в корпоративной среде растёт год от года. Не подключённый виртуальный диск доступен в виде одного файла-контейнера, поэтому может переноситься на другие компьютеры и использоваться там, где это необходимо.

Чтобы этот рабочий процесс был безопасным, мы сделали следующее:

- реализовали прозрачное шифрование данных виртуального диска наиболее стойкими криптографическими алгоритмами ГОСТ 34.12-2018 и ГОСТ 34.13-2018;
- усилили защиту обязательной двухфакторной аутентификацией на основе ключевых контейнеров пользователей (ГОСТ 34.10-2018, ГОСТ 34.11-2018).

По нашей собственной статистике, среди клиентов, применяющих Secret Disk в среде Windows зашифрованные виртуальные диски - одна из самых популярных фич продукта. Функция реализована по аналогии с Secret Disk для Windows, это позволяет пользователям быстрее адаптироваться к переходу на Linux.

Управление защищёнными виртуальными дисками не требует глубоких компетенций в области защиты информации и не влияет на рабочие сценарии пользователей при переезде на новую рабочую станцию с ОС на базе Linux. Все настройки осуществляются традиционным для администратора способом, через интуитивно понятный графический интерфейс. Также для администраторов Linux предусмотрен классический способ настройки защиты через командную консоль, что дает дополнительные возможности автоматизации процесса при выполнении масштабных задач.

Наши рекомендации по безопасному переходу с Windows на Linux

Для того, чтобы начать осваиваться в новой реальности и организовать гетерогенную инфраструктуру Windows-Linux необходимо сделать три простых шага:

- На той части рабочих компьютеров под Windows, где хранится важная, чувствительная к утечке информация заместить встроенное средство шифрования Bitlocker на надёжные решения. В первую очередь это необходимо для того, чтобы обезопасить информацию от компрометации (данное встроенное средство обладает низкой криптостойкостью) и непредсказуемых действий со стороны разработчика Microsoft. Для этого подойдет Secret Disk 5 и Secret Disk Enterprise.

- На новых рабочих станциях с ОС на базе Linux разместить конфиденциальные данные в безопасном рабочем пространстве – зашифрованном виртуальном диске, созданном с помощью Secret Disk для Linux. Таким образом, информационные активы, наиболее подверженные риску утечки будут находиться в безопасном и импортонезависимом сегменте инфраструктуры.

- Перейти к реорганизации других, более сложных элементов ИТ-инфраструктуры.

Secret Disk для Linux – алгоритм создания защищённого рабочего пространства

Как мы уже говорили ранее, управление Secret Disk для Linux осуществляется с помощью командной строки и через web-интерфейс. В данном документе фокус внимания будет сделан на работе с графическим интерфейсом. Для ознакомления с работой в консоли необходимо обратиться к Руководству администратора.

Итак, создание защищённого рабочего пространства состоит из следующих этапов:

1. Запуск графического интерфейса.

2. Выпуск для пользователя виртуального аутентификатора (далее ключевой контейнер пользователя или ККП).

3. Создание учётной записи пользователя и присвоение ему его личного ККП.

4. Создание защищённого виртуального диска.

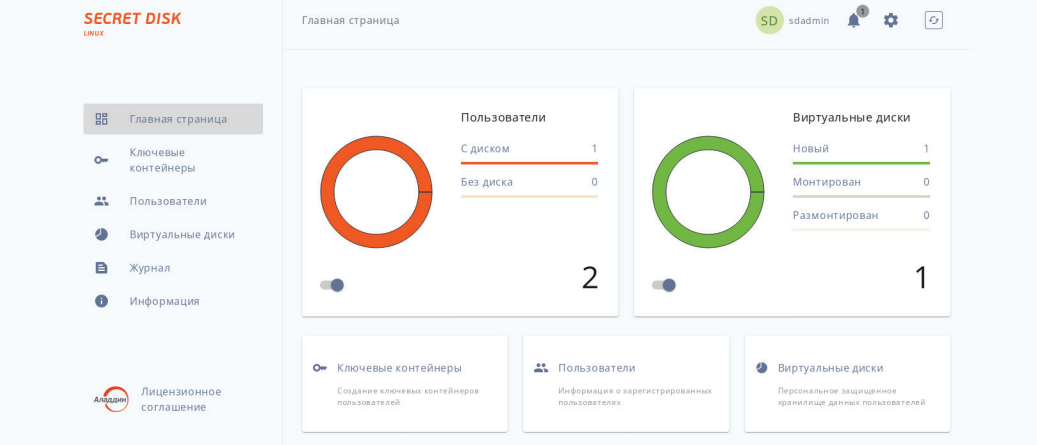
Рассмотрим подробнее весь процесс.

1. Запуск графического интерфейса

Чтобы запустить графический интерфейс нужно единожды воспользоваться командной строкой и установить инсталляционные файлы.
Запускаем web-приложение Secret Disk для Linux - открываем сессию для Администратора с параметром -w

```
[sdadmin@localhost ~]$ sdopen -w
Пароль:
Успешно
```

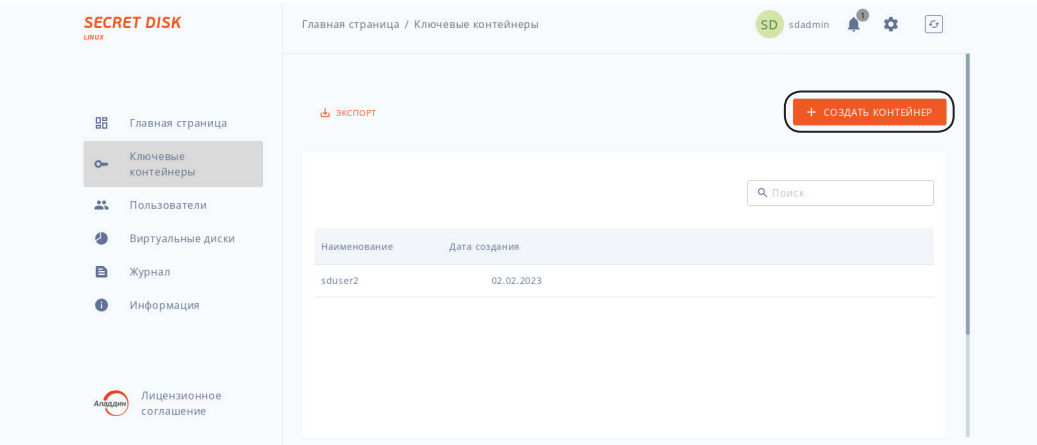
После авторизации Администратор попадает на главную страницу web-приложения, где представлены основные дашборды. Дашборды показывают общую картину пользователей и состояние их виртуальных дисков.



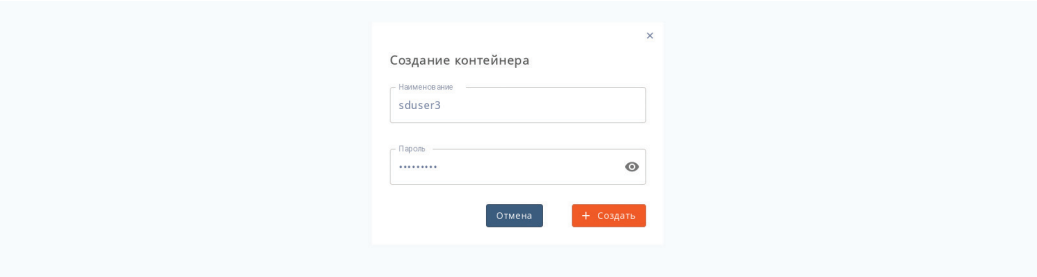
2. Выпуск виртуального аутентификатора

Чтобы приступить к созданию виртуального диска в Secret Disk для Linux, в первую очередь необходимо сначала выпустить виртуальный аутентификатор для пользователя. Виртуальный аутентификатор – это ключевой контейнер пользователя (ККП). ККП создает Администратор, передает его пользователю и после этого более не имеет к нему доступа.

- Для создания ККП переходим в раздел Ключевые контейнеры.
  Далее нажимаем на кнопку СОЗДАТЬ КОНТЕЙНЕР в правом верхнем углу.



- Далее заполняем форму данных для создания ККП и подтверждаем его создание.

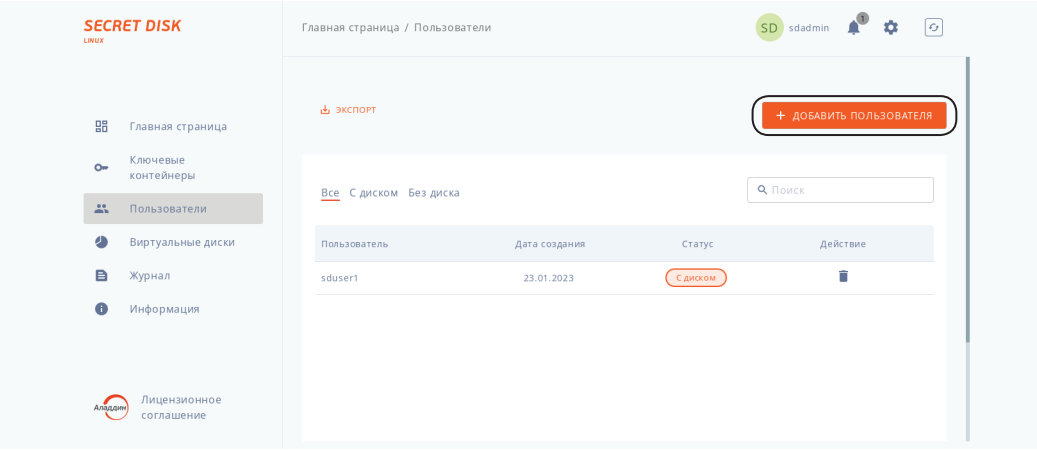


Готово!

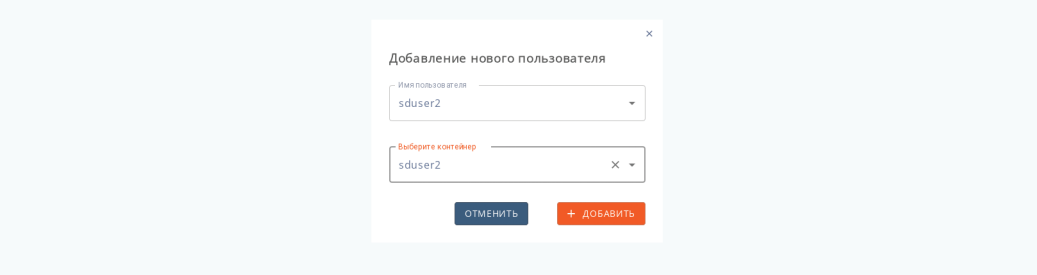
Теперь переходим к созданию пользователя.

3. Создание учётной записи пользователя

- Для создания пользователя Secret Disk для Linux нажимаем на кнопку ДОБАВИТЬ ПОЛЬЗОВАТЕЛЯ в правом верхнем углу.



- Заполняем данные в открывшемся окне. Обязательно присваиваем пользователю один из созданных ранее ККП в поле Выберите контейнер.



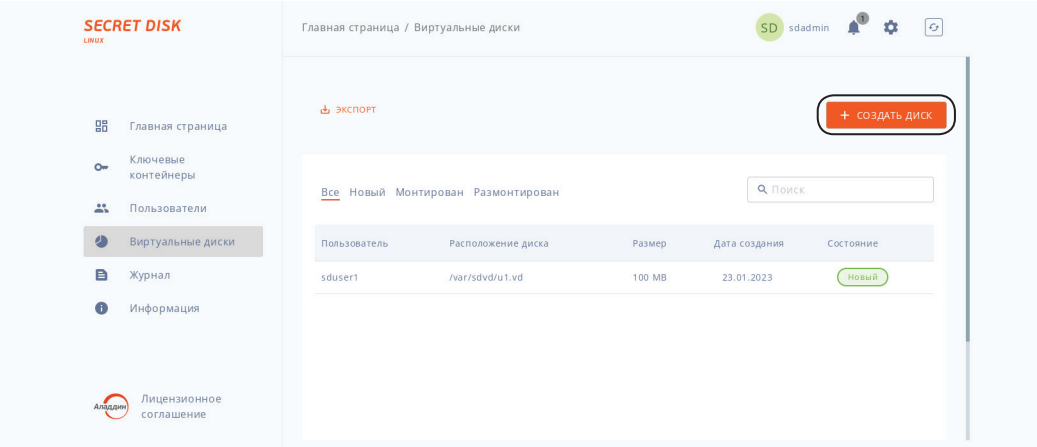
ВАЖНО!

После того, как ККП был присвоен пользователю, он автоматически исчезает из панели управления и становится недоступным для Администратора.

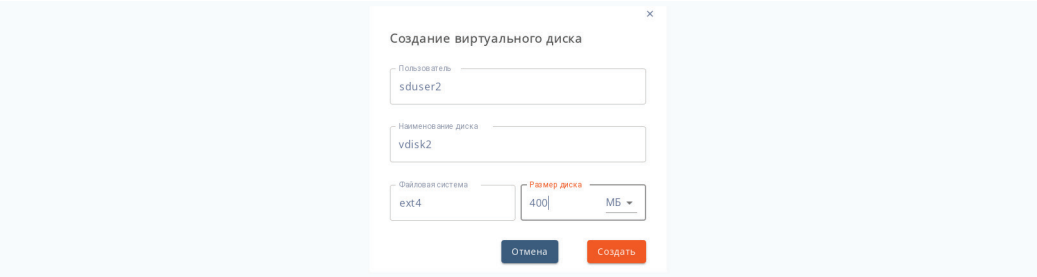
Теперь все готово для создания виртуального диска.

4. Создание защищённого виртуального диска

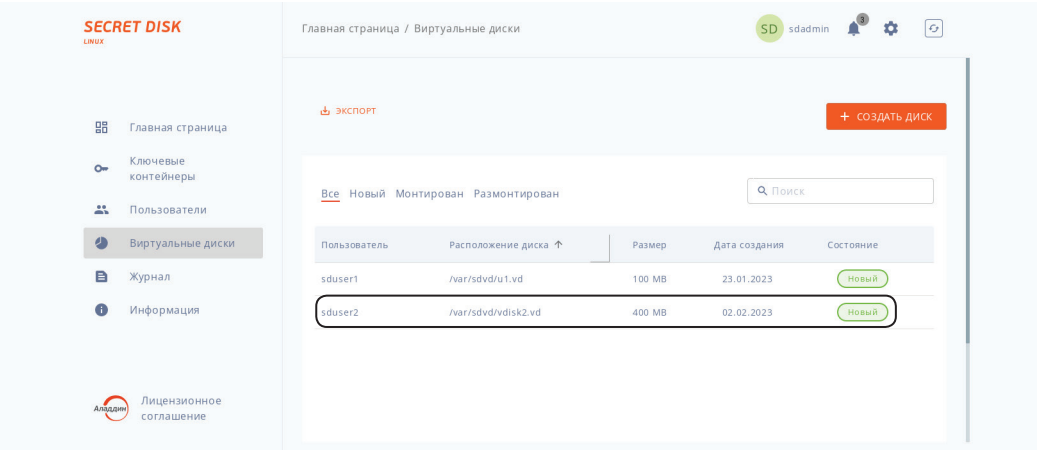
- Для создания защищённого виртуального диска нажимаем на кнопку СОЗДАТЬ ДИСК, расположенную в правом верхнем углу.



- Затем заполняем данные в соответствующей форме.

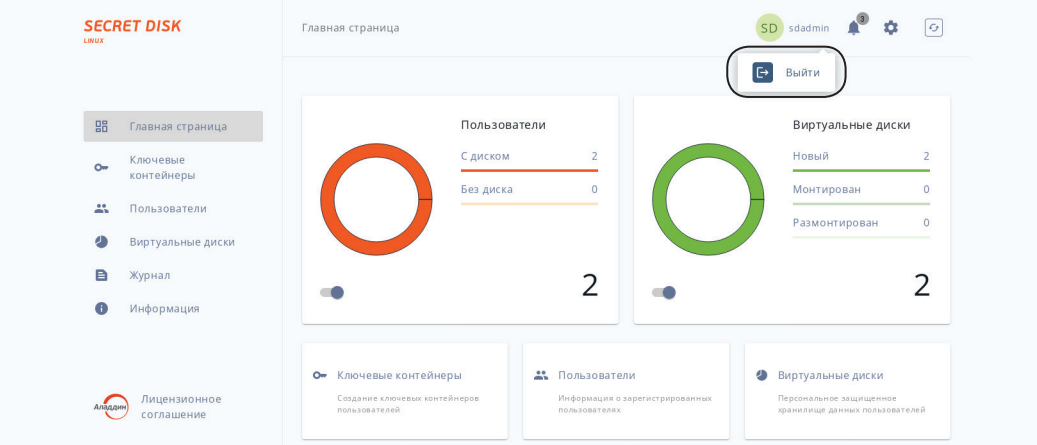


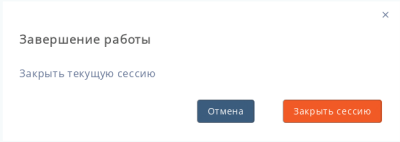
Готово!
Созданный диск появился в таблице с виртуальными дисками.



Работа завершена.

Чтобы завершить сессию Администратора последовательно нажимаем кнопки Выйти – > Закрыть сессию





ВАЖНО!

В целях безопасности повторно открыть сессию можно только в командной строке.

+7 (495) 223-00-01
aladdin@aladdin.ru
www.aladdin.ru

AladdinRD